

Descent for the punctured universal elliptic curve, and the average number of integral points on elliptic curves

Dohyeong Kim

December 8, 2015

Abstract

We show that the average number of integral points on elliptic curves, counted modulo the natural involution on a punctured elliptic curve, is bounded from above by 2.1×10^8 . To prove it, we design a descent map, whose prototype goes at least back to Mordell, which associates a pair of binary forms to an integral point on an elliptic curve. Other ingredients of the proof include the upper bounds for the number of solutions of a Thue equation by Evertse and Akhtari-Okazaki, and the estimation of the number of binary quartic forms by Bhargava-Shankar. Our method applies to S -integral points to some extent, although our present knowledge is insufficient to deduce an upper bound for the average number of them. We work out the numerical example with $S = \{2\}$.

Contents

1	Introduction	2
2	Two binary forms associated to a point on an elliptic curve	4
3	Equivalence between pairs of binary forms.	9
4	Descent for the S -integral points on the punctured universal elliptic curve	12
5	The example $S = \{2\}$	14
6	The average number of integral points on elliptic curves	16

1 Introduction

The goal of the present article is to show that the average number of integral points on the curves

$$Y_{a,b}: y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}, \quad 4a^3 + 27b^2 \neq 0 \quad (1)$$

is bounded from above by 2.1×10^8 . The points are counted modulo the natural involution $(x, y) \mapsto (x, -y)$, which is of course equivalent to the negation with respect to the group law of the underlying elliptic curve. The average is taken with respect to the height

$$H(Y_{a,b}) := \max \{2^{12}3^4|a|^3, 2^{14}3^{12}b^2\} \quad (2)$$

where the reasons behind the numbers multiplied to $|a|^3$ and b^2 are to be explained later.

Although our primary interest lies in the curves in the form (1), we will develop some techniques that are applicable to a slightly wider range of equations. Namely, we will consider any curve

$$Y: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z} \quad (3)$$

in a generalised Weierstrass equation, and study the set of S -integral points on it, where S is a finite set of prime numbers. We always assume that Y/\mathbb{Q} is nonsingular. Our main strategy is to reduce the study of S -integral points on the curve of the form (3) to that of solutions of certain quartic Thue-Mahler equations.

In fact, the above strategy is not entirely new; the possibility of such a reduction was known at least to Mordell. In Chapter 27 of his book [7], he proves that the set of integral solutions of the equation

$$ey^2 = ax^3 + bx^2 + cx + d, \quad a, b, c, d, e \in \mathbb{Z} \quad (4)$$

is finite, under the assumption that the cubic polynomial on the right hand side does not have repeated roots, by reducing it to the combination of two finiteness results on the number of binary quartic forms with given invariants and the number of solutions of a quartic Thue equation. More precisely, Mordell showed that x and z coordinates of the affine surface

$$ey^2 = ax^3 + bx^2z + cxz^2 + dz^3 \quad (5)$$

can be parametrised by a pair of explicit quartic forms. Geometrically speaking, it shows that the above affine surface is unirational. Perhaps some readers might be reminded about the well known result which says that any smooth cubic surface is geometrically rational.

In our approach, a key role is played by an explicit map, called the descent map, which is generically an isomorphism between open subsets of two GIT type spaces. One is the universal elliptic curve modulo the natural involution, and

the other is the orbit space of pairs of binary forms of degree 1 and 4. The S -integral points on elliptic curves are parametrised by the complement of the zero section of the universal elliptic curve, namely the punctured universal elliptic curve, while the binary quartic forms together with a solution of its associated Thue-Mahler equation are parametrised by an open subset of the latter.

It turns out that the binary quartic form that we associate to a point on an elliptic curve via the descent map is equivalent to the quartic form which is used by Mordell in order to parametrise the z -coordinate of the affine surface (5). In some sense, our method is essentially that of Mordell, and our contribution is to appropriately repackage his method so that it is suitable for our purpose, and that one can connect it to a few deep results that could not have been available to him.

Having established the descent map in an appropriate form, the average number of integral points on curves of the form $Y_{a,b}$ can be obtained without too much difficulty. Indeed, the work [5] of Bhargava-Shankar provides the asymptotic growth of the average number of integral binary quartic forms with given invariants, and the works [1, 3] of Akhtari-Okazaki and Evertse provide absolute upper bounds for the number of solutions of a quartic Thue equation. Combining these, we will be able to prove the desired upper bound. In fact, the normalisation of $H(Y_{a,b})$ is chosen in a way which is compatible with the choice made by Bhargava-Shankar.

We give a brief discussion on our terminology. The equations (1) and (3) have underlying (projective) elliptic curves, and their \mathbb{Z}_S -solutions may be abusively called as \mathbb{Z}_S -points on those elliptic curves. Here, an S -integral point on an elliptic curve should be understood as a scheme theoretic \mathbb{Z}_S -point on the punctured elliptic curve. Of course, the notion of S -integral points coincides with that of rational points for a projective curve, and the study of S -integral points is meaningful only for the punctured elliptic curve. Since the rational points on an elliptic curves are not our current subject matter, our abuse of terminology should not cause too much confusion.

Going back to our discussion on the technical aspects of the present article, note that our argument does not involve the ranks of elliptic curves, nor the arithmetic invariants of some auxiliary number fields. To the best knowledge of the author, the previously known bounds for the number of integral points on a particular elliptic curve depend exponentially either on the rank of the curve, or the rank of certain ideal class group of a number field such as the two-division field of the curve. Combining this type of upper bounds with an analysis on the distribution of ranks, one might try to obtain an upper bound for the average number of points on elliptic curves. Indeed, Alpoge [2] considered a family, which is almost but not exactly identical to ours, of elliptic curves, and claimed that this strategy yields 65.8457 as an upper bound. His family consists of the curves $Y_{a,b}$ as above, but with an additional condition that $Y_{a,b}$ is minimal; there is no prime p such that both $p^4|a$ and $p^6|b$ hold.

As we mentioned earlier, the descent map is generically an isomorphism, and this has an implication about S -integral points on elliptic curves. In fact, the descent map turns out to be an isomorphism over $\mathbb{Z}[1/6]$. If an elliptic

curve E/\mathbb{Q} has good reduction outside S , then the S -integral points on E can be defined using the smooth model of E over \mathbb{Z}_S , the ring of S -integers. Let us temporarily denote by E an elliptic curve over \mathbb{Q} which has good reduction outside S , and by t a \mathbb{Z}_S -point on E minus the origin. Using the descent map, we will obtain a bijection between the set of all equivalence classes of pairs (E, t) and the set of orbits of pairs of binary forms, provided that both 2 and 3 are contained in S . For arbitrary S , the descent map does not necessarily induce a bijection, but it remains to be injective, whence it can be used to compute all such pairs (E, t) . We numerically demonstrate this for $S = \{2\}$.

We outline the organisation of the paper. In Section 2, we define the descent map, which associates two integral binary forms to a point on the punctured universal elliptic curve. In Section 3, we review some basic properties of the notion of equivalence between pairs of binary forms. In Section 4, we use the descent map to identify S -integral points on the punctured universal elliptic curve with certain equivalence classes of pairs of binary forms. In Section 5, we work out the numerical example with $S = \{2\}$. In Section 6, we use the descent map together with the works of Akhtari-Okazaki, Evertse, and Bhargava-Shankar to establish the desired upper bound for the average number of integral points on elliptic curves.

We close the introduction with two remarks. Firstly, one naturally wonders what can be done on the average number of S -integral points on elliptic curves. An obstacle is placed by the fact that the result of Bhargava and Shankar is restricted to the binary forms with integer coefficients with respect to $\mathrm{GL}_2(\mathbb{Z})$ transformation, rather than forms with coefficients in \mathbb{Z}_S that are subject to $\mathrm{GL}_2(\mathbb{Z}_S)$ -transformations. On the other hand, the descent map exists without any restriction of S , and Theorem 6.3 is extended to the forms with S -integral coefficients in [4] with an upper bound which is independent of the form. Secondly, one also wonders what would be the true average number of integral points, if exists, on curves of the form $Y_{a,b}$. While we are relying on the absolute upper bound for the number of solutions of a Thue equation, namely Theorem 6.4, the average number of solutions of a Thue equation may well be smaller. If so, one might hope to improve our present upper bound.

Acknowledgement

This work was supported by IBS-R003-D1.

2 Two binary forms associated to a point on an elliptic curve

The aim of the present section is to define two integral binary forms associated to a point on an elliptic curve, and study its basic properties.

We begin with notations. Let E

$$E: y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \quad (6)$$

be an elliptic curve written in a generalised Weierstrass equation whose coefficients are rational integers. If t is a \mathbb{Z} -point of E , then we shall write

$$t = (x_t : y_t : z_t) \quad (7)$$

where x_t, y_t , and z_t are relatively prime integers.

Let Y be the elliptic curve punctured at the origin. In other words, Y is the open subscheme of E defined by the complement of the vanishing locus of z . If S is any finite set of primes, we denote by \mathbb{Z}_S the ring of S -integers. Then, \mathbb{Z}_S -points of Y can be described as

$$Y(\mathbb{Z}_S) = \{t = (x_t : y_t : z_t) : t \in E(\mathbb{Z}), z_t \in \mathbb{Z}_S^\times\}. \quad (8)$$

Of course, the points of $Y(\mathbb{Z}_S)$ bijectively correspond to the solutions of the affine equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (9)$$

so one can view (8) as an alternative description for the set of solutions of (9) in \mathbb{Z}_S . In our exposition, we will mainly use (8).

For each point $t \in Y(\mathbb{Z}_S)$, we will construct two binary forms of degree one and four respectively. We denote them by L_t and Q_t , where the letters are chosen to suggest that they are linear and quartic forms, respectively. The variables of L_t and Q_t will be denoted by u and v , so we shall often write $L_t(u, v)$ and $Q_t(u, v)$ in order to emphasise the variables. We explain the construction of $L_t(u, v)$ and $Q_t(u, v)$ below.

The construction of L_t is straightforward. Independently of t , we let

$$L_t(u, v) = v \quad (10)$$

which is regarded as a linear form in variables u and v . For the geometric reason underlying this hardly motivating definition, see Remark 2.1

The construction of Q_t is slightly more involved, though it is a classical one which is often used in two-descent for elliptic curves. Let \mathbb{P}_{xyz}^2 be the projective plane with homogeneous coordinates x, y , and z . Note that E is given as a cubic curve in \mathbb{P}_{xyz}^2 . For a given $t \in Y(\mathbb{Z}_S)$, the lines in \mathbb{P}_{xyz}^2 which passes through t are (projectively) parametrised by the linear forms

$$ux + vy + wz = 0 \quad (11)$$

such that

$$ux_t + vy_t + wz_t = 0 \quad (12)$$

is satisfied. Under the assumption that $z_t \neq 0$, such lines are parametrised by u and v , because we can uniquely recover w

$$w = \frac{ux_t + vy_t}{-z_t} \quad (13)$$

from u and v .

The quartic form $Q_t(u, v)$, which will be determined explicitly shortly, is characterised by the property that its four zeros represent the four lines which are the ramification points of the projection map from E to the space of lines through t .

Proposition 2.1. *The quartic form $Q_t(u, v)$ is given by*

$$A^2 - 4v^2B \quad (14)$$

where A and B are given as

$$A = -z_t u^2 + z_t a_1 uv + (a_2 z_t + x_t) v^2 \quad (15)$$

$$B = x_t z_t u^2 + (2y_t z_t + z_t^2 a_3) uv + (a_4 z_t^2 - a_1 z_t y_t + a_2 z_t x_t + x_t^2) v^2. \quad (16)$$

Proof. This follows from a straightforward calculation. We need to find the algebraic condition that is equivalent to the geometric one that the line

$$ux + vy + wz = 0 \quad (17)$$

is tangent to E . We substitute

$$y = \frac{ux + wz}{-v} \quad (18)$$

to

$$y^2 z + a_1 xyz + a_3 yz^2 - (x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3) \quad (19)$$

and obtain a cubic form $C(x, z)$ in x and z . Using the condition that t satisfies both (17) and (19), one observes that $C(x, z)$ should have a factorisation

$$C(x, z) = \frac{1}{z_t v^2} (xz_t - zx_t) \cdot q(x, z) \quad (20)$$

where $q(x, z)$ is a quadratic form in x and z whose coefficients are quadratic in u and v . By expanding the right hand side of (20) and equating the coefficients of it with those of $C(x, z)$, one obtains

$$q(x, z) = v^2 x^2 + Axy + By^2 \quad (21)$$

where A and B are polynomials given in the statement of the proposition. The condition that the line is ramification point of the projection map is equivalent to the condition that the discriminant of $q(x, z)$ is zero. From this, one obtains the formula of $Q_t(u, v)$. \square

Remark 2.1. The linear form $L_t(u, v) = v$ acquires the following geometric interpretation once we view u and v as parameter for the lines passing through t . The zero of $L_t(u, v)$ is $(u, v) = (1, 0)$, which corresponds to the line

$$x - \frac{x_t}{z_t} z = 0 \quad (22)$$

passing through t and the origin of E .

Remark 2.2. In the context of two-descent for the elliptic curve E , $Q_t(u, v)$ represents a torsor for $E[2]$, the group of two division points of E .

Let us work out some numerical examples in order to ensure that the formula of $Q_t(u, v)$ is correct and to illustrate the nature of $Q_t(u, v)$. Let us consider

$$E: y^2z + yz^2 = x^3 - xz^3 \quad (23)$$

which is the curve of conductor 37. It has no non-trivial rational point of order two. Its rank is one, and the Mordell-Weil group is generated by the point

$$P_0 = (0, 0, 1). \quad (24)$$

Let us take $t = n \cdot P$.

For $n = 1$, one gets

$$Q_t(u, v) = u^4 - 4uv^3 + 4v^4 \quad (25)$$

which is irreducible.

For $n = 2$, we have $t = (1, 0, 1)$. One readily computes that

$$Q_t(u, v) = u^4 - 6u^2v^2 - 4uv^3 + v^4 \quad (26)$$

which factors as

$$(u + v)(u^3 - u^2v - 5uv^2 + v^3) \quad (27)$$

verifying that the corresponding torsor is trivial.

For $n = 3$, we have $t = (-1, -1, 1)$. Similarly, we have

$$Q_t(u, v) = u^4 + 6u^2v^2 + 4uv^3 + v^4 \quad (28)$$

which is irreducible.

As a second example, consider

$$E: y^2z = x^3 - 1681xz^2. \quad (29)$$

Since $1681 = 41^2$ is a square, it has three rational points of order two. Also, it turns out that the Mordell-Weil group has rank two, generated by

$$P_1 = (-9, 120, 1) \quad (30)$$

$$P_2 = (841, 24360, 1). \quad (31)$$

For $t = P_1$, we have

$$Q_t(u, v) = u^4 + 54u^2v^2 - 960uv^3 + 6481v^4 \quad (32)$$

which is irreducible.

For $t = P_2$, we have

$$Q_t(u, v) = u^4 - 5046u^2v^2 - 194880uv^3 - 2115119v^4 \quad (33)$$

which factors as

$$(u^2 - 58uv - 2521v^2)(u^2 + 58uv + 839v^2) \quad (34)$$

but does not possess a linear factor.

For $t = 2 \cdot P_1$, one has

$$t = (93139320, 443882159, 1728000) \quad (35)$$

and

$$Q_t(u, v) = 43200(40u - 827v)(120u + 143v)(120u + 719v)(120u + 1619v). \quad (36)$$

It verifies that $Q_t(u, v)$ defines the trivial torsor as expected.

Now we turn to the key proposition regarding both $L_t(u, v)$ and $Q_t(u, v)$.

Proposition 2.2. *Let Δ_E be the discriminant of E , and let S be any finite set of primes numbers. Let Δ_t be the discriminant of binary quintic form $L_t(u, v) \cdot Q_t(u, v)$. Then Δ_t is a unit in $\mathbb{Z}_S[(2\Delta_E)^{-1}]$.*

Proof. Let p be an odd prime such that p does not divide Δ_E and p does not belong to S . In order to prove the proposition, it suffices to show that Δ_t is prime to p . We proceed in two steps.

Firstly, we will show that the discriminant of $Q_t(u, v)$ is prime to p . Let $t \in Y(\mathbb{Z}_S)$, and let t_p be the reduction of t modulo p . Let E_p be the reduction of E modulo p . Consider the twisted multiplication-by-two map

$$\theta: E_p \rightarrow E_p \quad (37)$$

$$s \mapsto -2s \quad (38)$$

which is a separable morphism since p is odd. Also, the degree of θ is four. It follows that

$$\theta^{-1}(t_p) \quad (39)$$

has four geometric points. Connecting the four geometric points with t_p , we obtain four lines passing through t_p , and these four lines are precisely represented by the zeroes of $Q_t(u, v)$ modulo p . The non-vanishing of the discriminant of $Q_t(u, v)$ modulo p is equivalent to the condition that four lines are distinct. Suppose that two of the four lines coincide, say L_0 . Then L_0 contains $s_1, s_2 \in \theta^{-1}(t_p)$ which are distinct. Furthermore, L_0 is tangent to E_p at s_1 and s_2 by construction. This contradicts that L_0 and E_p intersects with multiplicity three, and we completed the proof of the first step, showing that the discriminant of $Q_t(u, v)$ is prime to p .

Now we proceed to the second step. It is based on the representation of the discriminant as a product of root differences. Indeed, if we let δ_t be the discriminant of Q_t , then one finds that

$$\Delta_t = \delta_t \cdot Q_t(1, 0)^2 \quad (40)$$

from the representation of the discriminant as square of the product of all possible differences between roots. In the first step, we showed that δ_t is prime to p , so it remains to show that $Q_t(1, 0)$ is prime to p . This follows immediately from our explicit formula for $Q_t(u, v)$ given in Proposition 2.1, from which we see the number

$$Q_t(1, 0) = z_t^2 \quad (41)$$

is prime to p if $t \in Y(\mathbb{Z}_S)$. \square

The argument using the dull algebraic identity (40) can be replaced with the following geometric argument. That is to say, we would like to show geometrically that any of the four lines defined by $Q_t = 0$ equals the line defined by $L_t = 0$, after taking the reduction modulo p . Let us begin with the following lemma.

Lemma 2.1. *None of the four geometric points belonging to $\theta^{-1}(t_p)$ is the origin of E_p .*

Proof. Indeed, suppose on the contrary that s is a geometric point of $\theta^{-1}(t_p)$ and s is the origin of E_p . Then $\theta(s) = t_p$ implies, by definition of θ , that

$$-2s = t_p, \quad (42)$$

which implies $t_p = 0$. It contradicts that t_p is not the origin of E_p . This observation in turn implies that none of the four lines defined by the zeros of $Q_t(u, v)$ modulo p passes through the origin. \square

Suppose, on the contrary, that there is a line L_0 which passes through one of the four points of $\theta^{-1}(t_p)$, say s_0 , and further passes through both t_p and the origin. Note that s_0 cannot be the origin by the lemma. It follows that L_0 meets E_p with multiplicity at least five, to which the origin contributes at least three, and s_0 together contributes two. It is absurd.

3 Equivalence between pairs of binary forms.

There are several notions for equivalence between pairs of binary forms. The aim of the current section is to define the notion of equivalence which is relevant to our purpose.

Let S be any finite set of primes. Let us consider a pair (L, Q) of binary forms

$$L = b_0u + b_1v \quad (43)$$

$$Q = c_0u^4 + c_1u^3v + c_2u^2v^2 + c_3uv^3 + c_4v^4 \quad (44)$$

where b_i 's and c_i 's are S -integers. We always assume that the coefficients of L and Q do not have non-trivial common divisors in \mathbb{Z}_S . More precisely, we assume

that the ideal of \mathbb{Z}_S generated by b_0 and b_1 is the unit ideal, and similarly the ideal of \mathbb{Z}_S generated by c_0, c_1, \dots, c_4 is also the unit ideal.

The discriminant of Q , denoted by Δ_Q , is given by

$$\begin{aligned} \Delta_Q = & c_1^2 c_2^2 c_3^2 - 4c_0 c_2^3 c_3^2 - 4c_1^3 c_3^3 + 18c_0 c_1 c_2 c_3^3 - 27c_0^2 c_3^4 - 4c_1^2 c_2^3 c_4 \\ & + 16c_0 c_2^4 c_4 + 18c_1^3 c_2 c_3 c_4 - 80c_0 c_1 c_2^2 c_3 c_4 - 6c_0 c_1^2 c_3^2 c_4 + 144c_0^2 c_2 c_3^2 c_4 \\ & - 27c_1^4 c_4^2 + 144c_0 c_1^2 c_2 c_4^2 - 128c_0^2 c_2^2 c_4^2 - 192c_0^2 c_1 c_3 c_4^2 + 256c_0^3 c_4^3 \end{aligned} \quad (45)$$

and the discriminant of $L \cdot Q$, denoted by Δ , is given by

$$\Delta = \Delta_Q \cdot Q(-b_1, b_0)^2. \quad (46)$$

For a fixed S , we will be concerned with pairs of forms for which Δ is an S -unit. We introduce the following notion of admissibility to simplify the exposition.

Definition 3.1. Let (L, Q) be a pair of binary forms with S -integral coefficients as above. We say that this pair of S -admissible if Δ is an S -unit.

Let (L, Q) and (L', Q') be two S -admissible pairs. There is, of course, the obvious notion of equality between them, defined by the coefficient-wise equality. A weaker notion of equality, which is more natural if we view them as elements of projective space, is the following.

Definition 3.2. Let (L, Q) and (L', Q') be two S -admissible pairs. We say that two pairs are projectively equivalent if there are

$$\lambda_1, \lambda_2 \in \mathbb{Z}_S^\times \quad (47)$$

such that

$$(L, Q) = (\lambda_1 L', \lambda_2 Q') \quad (48)$$

holds.

Note that this definition does make sense among S -admissible pairs, because if Δ is the discriminant of (L, Q) , then the discriminant of $(\lambda_1 L, \lambda_2 Q)$ is $\lambda_1^8 \lambda_2^2 \Delta$.

Now we introduce the desired notion of equivalence.

Definition 3.3. Let (L, Q) and (L', Q') be two S -admissible pairs. We say that they are GL_2 -equivalent, if there is $g \in \text{GL}_2(\mathbb{Z}_S)$ such that (L^g, Q^g) is projectively equivalent to (L', Q') . Here g acts on L and Q by the linear change of variables.

We would like to take a closer look at the notion of GL_2 -equivalence, under the assumption that $2 \in S$. If $2 \in S$, then for each S -admissible pair (L, Q) , it is possible to find a pair (L', Q') , which is GL_2 -equivalent form, such that

$$L' = v \quad (49)$$

$$Q' = u^4 + B_2 u^2 v^2 + B_3 u v^3 + B_4 v^4 \quad (50)$$

where B_2, B_3, B_4 are integers, rather than S -integers. Furthermore, it is possible, as we will prove shortly, to choose a minimal one in the following sense.

Definition 3.4. A pair of binary forms

$$(v, u^4 + B_2 u^2 v^2 + B_3 u v^3 + B_4 v^4) \quad (51)$$

with integral coefficient is called minimal, if there is no prime p such that $p^i | B_i$ for $i = 2, 3, 4$ simultaneously. If the form has S -integral coefficient, then it is called minimal at p for a prime $p \notin S$, when $p^i | B_i$ for $i = 2, 3, 4$ does not hold simultaneously.

Proposition 3.1. *Recall that 2 is contained in S . Given any pair (L, Q) of binary forms as above, it is possible to find a minimal pair*

$$(v, u^4 + B_2 u^2 v^2 + B_3 u v^3 + B_4 v^4) \quad (52)$$

which is GL_2 -equivalent to (L, Q) . Such a minimal pair is unique up to replacing B_3 with $-B_3$. In other words, such a minimal pair is unique if $B_3 = 0$, and there are precisely two such pairs if $B_3 \neq 0$.

Proof. The proof is by elementary algebra. Let (L, Q) be an S -admissible pair given by

$$L = b_0 u + b_1 v \quad (53)$$

$$Q = c_0 u^4 + c_1 u^3 v + c_2 u^2 v^2 + c_3 u v^3 + c_4 v^4. \quad (54)$$

Since b_0 and b_1 generate the unit ideal in \mathbb{Z}_S , by a linear change of variables, we may assume $L = v$. Then, c_0 must be S -unit. Otherwise,

$$Q(b_1, -b_0) = c_0 \quad (55)$$

divides Δ , contradicting the S -admissibility of the pair. Thus, via a projective equivalence, we may assume that $c_0 = 1$. Now we have a pair

$$L = v \quad (56)$$

$$Q = u^4 + c_1 u^3 v + c_2 u^2 v^2 + c_3 u v^3 + c_4 v^4. \quad (57)$$

where the coefficients are in \mathbb{Z}_S . Since we assumed $2 \in S$, we are allowed make the substitution

$$u \mapsto u - \frac{c_1}{4} v$$

if necessary, so we may assume that $c_1 = 0$ as well. Since the denominators of c_2, c_3, c_4 are S -units, we may multiply an S -unit to v , and apply projective equivalence, in order to get a minimal form.

The only linear change of variables which preserve the condition that Q is monic in u , $c_1 = 0$, and there is no prime p such that $p^i | c_i$ simultaneously, is

$$(u, v) \mapsto (\lambda_1 u, \lambda_2 v) \quad (58)$$

where λ_1 is a fourth root of unity, and λ_2 is a unit. Thus, all possible minimal pairs which is equivalent to a given minimal form

$$L = v \quad (59)$$

$$Q = u^4 + c_2 u^2 v^2 + c_3 u v^3 + c_4 v^4 \quad (60)$$

must be obtained by replacing c_3 with $-c_3$. The proof of the proposition is complete. \square

Remark 3.1. It is worth noting that if we work over a general number field, then the number of possible minimal forms may grow. However, the involution $c_3 \mapsto -c_3$ on the set of minimal forms maintains an exceptional importance, since it will correspond to the negation on the elliptic curve.

4 Descent for the S -integral points on the punctured universal elliptic curve

We apply the results from the previous sections in order to classify S -integral points on the universal elliptic curve. We denote by \mathcal{Y} the punctured universal elliptic curve, whose \mathbb{Z}_S points are given by

$$\mathcal{Y}(\mathbb{Z}_S) = \{(Y, P) : P \in Y(\mathbb{Z}_S), Y \text{ is punctured smooth elliptic curve over } \mathbb{Z}_S\} \quad (61)$$

where a smooth elliptic curve over \mathbb{Z}_S means an elliptic curve over \mathbb{Q} which has good reduction outside of S . Note that the \mathbb{Z}_S -points on a curve is defined using the smooth model.

There is obvious action of the group $\{\pm 1\}$ of order two on $\mathcal{Y}(\mathbb{Z}_S)$, given by

$$\pm 1 : (Y, P) \mapsto (Y, \pm P) \quad (62)$$

where the negation denotes the negation under the group law of the elliptic curve. As promised in the introduction, we will prove the following theorem in the present section.

Theorem 4.1. *Assume $2, 3 \in S$. There is a bijection*

$$\kappa : \mathcal{Y}(\mathbb{Z}_S) / \{\pm 1\} \longrightarrow \{S\text{-admissible pairs}\} / \sim \quad (63)$$

where \sim is the GL_2 -equivalence relation.

Proof. We will prove the assertion by constructing the inverse. Let

$$(v, u^4 + B_2 u^2 v^2 + B_3 u v^3 + B_4 v^4) \quad (64)$$

be an S -admissible pair, which is minimal away from S . In particular, B_2, B_3, B_4 are S -integers, and the discriminant

$$-4B_2^3 B_3^2 + 16B_2^4 B_4 - 27B_3^4 + 144B_2 B_3^2 B_4 - 128B_2^2 B_4^2 + 256B_4^3 \quad (65)$$

is an S -unit. By defining

$$x_t = -\frac{1}{6}B_2 \quad (66)$$

$$y_t = -\frac{1}{8}B_3 \quad (67)$$

$$a_4 = -\frac{1}{4}(B_4 + 3x_t^2) \quad (68)$$

$$a_6 = y_t^2 - x_t^3 - a_4x_t \quad (69)$$

we obtain a curve

$$E: y^2 = x^3 + a_4x + a_6 \quad (70)$$

which is defined over \mathbb{Z}_S , and has a point $t = (x_t, y_t)$. Note that we have to divide by 6 in order to get x_t , hence rely on the assumption that $2, 3 \in S$. We need to show that E has good reduction outside of S . By direct computation, the discriminant of E is given by

$$2^{-8} \cdot (-4B_2^3B_3^2 + 16B_2^4B_4 - 27B_3^4 + 144B_2B_3^2B_4 - 128B_2^2B_4^2 + 256B_4^3) \quad (71)$$

which is an S -unit by comparison to the formula (65) for the discriminant of $Q(u, v)$.

We need to verify that the association $(L, Q) \mapsto (E, P)$ is well-defined. As we observed earlier, there is an involution on the set of minimal pairs sending B_3 to $-B_3$. It is clear from the formula (67) that it corresponds to the involution $(E, P) \mapsto (E, -P)$. Thus we have constructed a section of κ , showing its surjectivity.

To see the injectivity of κ , recall that if $2, 3 \in S$, hence an elliptic curve E which has good reduction outside of S has a model of the form (70) which has good reduction outside of S , and there is no prime p for which $p^4|a_4$ and $p^6|a_6$. Starting with a model of E which is minimal outside of S , we will show that the pair $(L, Q) = \kappa(E, P)$ is minimal away from S . By the explicit formula of (L, Q) given in Proposition 2.1, we have

$$Q(u, v) = u^4 - 6x_tu^2v^2 - 8y_tuv^3 - (3x_t^2 + 4a_4)v^4 \quad (72)$$

and we claim that it is minimal away from S . Suppose on the contrary that there is a prime $p \notin S$ for which $Q(u, v)$ is not minimal. Since $2, 3 \in S$,

$$p^2|x_t \quad (73)$$

$$p^4|3x_t^2 + 4a_4 \quad (74)$$

from which we conclude that $p^4|a_4$. Furthermore, non-minimality at p implies $p^3|y_t$. However, by rewriting the equation of the elliptic curve in the form

$$a_6 = y_t^2 - x_t^3 - a_4x_t \quad (75)$$

one sees p^6 divides a_6 . This contradicts the minimality of E at p .

Thus we have shown that κ is bijection. \square

5 The example $S = \{2\}$

The aim of present section is to give a numerical example, in which one determines $\mathcal{Y}(\mathbb{Z}_S)/\{\pm 1\}$ from the knowledge of a set of representatives for all S -admissible pairs. Although we assumed $2, 3 \in S$ in Theorem 4.1, as long as numerical examples are concerned, the assumption $2, 3 \in S$ is not strictly necessary. Indeed, the map κ exists anyway, and for each S -admissible pair, one obtains a point of \mathcal{Y} defined over $\mathbb{Z}_S[6^{-1}]$. One can proceed to verify whether this point is in fact defined over \mathbb{Z}_S or not, and by collecting those with an affirmative answer, one obtains $\mathcal{Y}(\mathbb{Z}_S)/\{\pm 1\}$.

Despite of the fact that the finiteness theorem for the number of equivalence classes of S -admissible pairs is effective, determination of it in practice can be rather challenging. In this section, we use the work of N.P. Smart who computed the all reducible binary quintic whose discriminant and S -unit with $S = \{2\}$. All S -admissible pairs can be obtained from the work of Smart, by choosing all possible linear factors of each binary quintic.

Table 1 is a produced from Table 5 of [8], which contains all reducible binary quintic forms whose discriminant is a power of 2 up to sign. In [8], the table is titled to contain all reducible binary quintic forms with 2-power discriminant, which might cause unnecessary confusion that the table is restricted to forms with positive discriminant. Thus we chose the expression that the discriminant is a power of 2 up to sign, which is equivalent to saying that the discriminant is S -unit with $S = \{2\}$.

Table 1: Reducible quintics whose discriminant is a power of 2 up to sign

i	$f_i(u, v)$	i	$f_i(u, v)$
1	$u^4v + u^3v^2 + u^2v^3 + uv^4$	2	$2u^4v + 2u^3v^2 - u^2v^3 - uv^4$
3	$8u^5 - 6u^3v^2 + uv^4$	4	$2u^5 - 3u^3v^2 + uv^4$
5	$u^5 + 4uv^4$	6	$u^5 + 3u^3v^2 + 2uv^4$
7	$u^4v + 3u^2v^3 + 2v^5$	8	$u^5 + 2u^4v + 4u^3v^2 + 4u^2v^3 + 4uv^4$
9	$u^5 + 3u^4v + 2u^3v^2 + 2u^2v^3 + uv^4 - v^5$	10	$u^5 - 4uv^4$
11	$u^5 + 4u^4v + 4u^3v^2 + 8u^2v^3 + 4uv^4$	12	$u^5 - 4u^4v + 8u^2v^3 - 4uv^4$
13	$u^4v - 8u^3v^2 + 12u^2v^3 + 16uv^4 - 28v^5$	14	$u^5 + u^4v + uv^4 + v^5$
15	$u^5 + uv^4$	16	$u^5 + 12u^3v^2 + 4uv^4$
17	$u^4v - 2v^5$	18	$u^5 + u^4v - 2uv^4 - 2v^5$
19	$u^5 - 2uv^4$	20	$u^4v + 2v^5$
21	$u^5 + 2uv^4$	22	$3u^5 + 8u^4v + 4u^3v^2 + 4uv^4$
23	$4u^4v + 4u^2v^3 - 16uv^4 + 9v^5$	24	$u^5 - 4u^3v^2 + 2uv^4$
25	$u^5 + 2u^4v - 4u^3v^2 - 8u^2v^3 + 2uv^4 + 4v^5$	26	$u^4v - 4u^2v^3 + 2v^5$
27	$u^5 + u^4v - 4u^3v^2 - 4u^2v^3 + 2uv^4 + 2v^5$	28	$u^5 + 9u^4v + 14u^3v^2 - 34u^2v^3 - 19uv^4 + 5v^5$
29	$u^5 + 4u^4v - 6u^3v^2 - 4u^2v^3 + uv^4$	30	$4u^4v + 16u^3v^2 - 12u^2v^3 - 24uv^4 + 17v^5$
31	$4u^5 + 12u^4v - 28u^3v^2 - 12u^2v^3 + 41uv^4 - 17v^5$	32	$u^5 - 8u^4v + 4u^3v^2 + 16u^2v^3 + 4uv^4$
33	$u^5 - 7u^4v - 4u^3v^2 + 20u^2v^3 + 20uv^4 + 4v^5$	34	$u^5 + 4u^3v^2 + 2uv^4$
35	$u^4v + 4u^2v^3 + 2v^5$	36	$u^4v - 2u^2v^3 - v^5$
37	$u^5 + u^4v - 2u^3v^2 - 2u^2v^3 - uv^4 - v^5$	38	$u^5 - 2u^3v^2 - uv^4$
39	$u^5 + 4u^3v^2 - 4uv^4$	40	$u^4v + 4u^2v^3 - 4v^5$
41	$u^5 + u^4v + 4u^3v^2 + 4u^2v^3 - 4uv^4 - 4v^5$	42	$u^4v + 4u^3v^2 - 6u^2v^3 + 12uv^4 - 7v^5$
43	$u^5 + 3u^4v - 10u^3v^2 + 18u^2v^3 - 19uv^4 + 7v^5$	44	$u^5 - 2u^3v^2 + 2uv^4$
45	$u^4v - 2u^2v^3 + 2v^5$	46	$u^5 + u^4v - 2u^3v^2 - 2u^2v^3 + 2uv^4 + 2v^5$
47	$u^5 + 4u^3v^2 + 8uv^4$	48	$u^4v + 4u^2v^3 + 8v^5$
49	$5u^5 + 13u^4v + 2u^3v^2 - 14u^2v^3 - 3uv^4 + 5v^5$	50	$u^4v + 6u^2v^3 + 8uv^4 + 5v^5$
51	$u^5 + 4u^4v + 4u^3v^2 - 8u^2v^3 + 4uv^4$.	.

We wish to find all $\{2\}$ -admissible pairs (L, Q) from Table 1. For each (L, Q) ,

the quintic form $L \cdot Q$ must be equivalent to f_i for some i , hence we can find all of them by finding all possible factorisation of f_i into one linear and one quartic forms. In fact, f_i for $1 \leq i \leq 4$ has three linear factors, and the rest have a unique linear factor.

Let us work out the case of $i = 1$. In this case, $f_1(u, v)$ factors as

$$vu(u+v)(u^2+v^2) \quad (76)$$

hence there are three pairs

$$(v, u(u+v)(u^2+v^2)), (u, v(u+v)(u^2+v^2)), (u+v, uv(u^2+v^2)) \quad (77)$$

associated to $f_1(u, v)$. Applying $(u, v) \mapsto (v, u)$ one sees that the first two pairs are equivalent. Transforming them into minimal forms, we obtain two pairs

$$(L_1, Q_1) = (v, u^4 + 10u^2v^2 + 40uv^3 - 51v^4) \quad (78)$$

$$(L_2, Q_2) = (v, u^4 - v^4) \quad (79)$$

in their minimal forms. From (L_1, Q_1) , we obtain curve

$$E_1: y^2 = x^3 + \frac{32}{3}x + \frac{1280}{27} \quad (80)$$

with point

$$t = \left(-\frac{5}{3}, -5\right) \quad (81)$$

on it. Above model is not minimal at 3. The minimal equation for E_1 is

$$E_{128a1}: y^2 = x^3 + x^2 + x + 1 \quad (82)$$

whose label in Cremona's Elliptic Curve Database is "128a1", and the coordinates of t are

$$t = \left(-\frac{3}{4}, \frac{5}{8}\right) \quad (83)$$

with respect to the minimal equation.

Similarly, from (L_2, Q_2) we obtain the curve

$$y^2 = x^3 + \frac{1}{4}x \quad (84)$$

and the point $t = (0, 0)$. Above equation is has minimal equation

$$E_{32a1}: y^2 = x^3 + 4x \quad (85)$$

whose label is "32a1", and t has the same coordinate $t = (0, 0)$ with respect to the minimal equation.

In fact, E_{128a1} has more 2-integral points, one finds the list

$$(-1, 0, 1), (-3/4, 5/8, 1), (0, 1, 1), (1, 2, 1), (7, 20, 1) \quad (86)$$

by applying the command "S_integral_points" in SAGE. Note that the list shows S -integral points modulo the action of $\{\pm 1\}$ on the curve. We already produced the second point using f_1 , and one should be able to determine the rest using the remaining f'_i s. Indeed, the four remaining points can be obtained from $i = 11, 37, 40, 41$.

By carrying out similar calculations for all f_i , we obtain Table 2. We note the reader that f_{30} and f_{31} give rise to two equivalent pairs, and f_{42} and f_{43} give rise to two equivalent pairs as well.

Table 2: Correspondence between f_i 's and elliptic curves

Label	i	Label	i	Label	i
"128a1"	1, 11, 37, 40, 41	"128a2"	2, 4, 23, 32, 33, 45, 46	"128b1"	36
"128b2"	48	"128c1"	39	"128c2"	47
"128d1"	38	"128d2"	44	"256a1"	2, 22, 24, 25, 51
"256a2"	3, 8, 27, 35	"256b1"	2, 21, 28, 29, 50	"256b2"	9, 17, 18
"256c1"	19	"256c2"	20	"256d1"	34
"256d2"	26	"32a1"	1, 42, 43	"32a2"	5, 12, 14
"32a3"	7	"32a4"	4, 49	"64a1"	13, 15, 16
"64a2"	6	"64a3"	3, 30, 31	"64a4"	10

6 The average number of integral points on elliptic curves

In this section, we shift our attention to the main goal of the paper, namely the average number of integral points on elliptic curves. Recall that we are considering the curves of the form

$$Y_{a,b}: y^2 = x^3 + ax + b \quad (87)$$

such that $a, b \in \mathbb{Z}$ and $4a^3 + 27b^2 \neq 0$. The curves $Y_{a,b}$ will be ordered by the height, normalised in the following way.

Definition 6.1. Define the height of $Y_{a,b}$, denoted by $H(Y_{a,b})$ as

$$H(Y_{a,b}) = \max\{2^{12}3^4|a|^3, 2^{14}3^{12}b^2\}. \quad (88)$$

Lemma 6.1. *Let T be a positive real. The number of curves $Y_{a,b}$ up to height T is asymptotically*

$$2^{-11}3^{-22/3}T^{5/6} < 1.55 \times 10^{-7} \times T^{5/6}.$$

Proof. It follows from the observation that there are $O(T^{1/3})$ pairs (a, b) satisfying $4a^3 + 27b^2 = 0$ and $\max\{2^{12}3^4|a|^3, 2^{14}3^{12}b^2\} < T$. \square

For any positive number T , define

$$N(T) = \sum_{Y_{a,b}, H(Y_{a,b}) < T} \sum_{t \in Y_{a,b}(\mathbb{Z})/\{\pm 1\}} 1 \quad (89)$$

which is the total number of integral points on the curves of the form $Y_{a,b}$ up to height T , counted modulo the action of $\{\pm 1\}$.

Theorem 6.1. *We have*

$$N(T) < (31.5 \dots) T^{5/6} \quad (90)$$

for all sufficiently large $T > 0$. In particular, the average number of integral points on curves of the form $Y_{a,b}$ is bounded by 2.1×10^8 . It is counted modulo the natural involution on the underlying elliptic curves.

In the rest of the section, we give the proof for Theorem 6.1. The starting point is a map

$$\phi: (Y_{a,b}, t) \mapsto ((1, 0), Q_{a,b,t}(u, v)) \in \mathbb{Z}^2 \times \text{Sym}^4(\mathbb{Z}^2)^* \quad (91)$$

where

$$Q_{a,b,t}(u, v) = u^4 - 6x_t u^2 v^2 - 8y_t u v^3 - (3x_t^2 + 4a)v^4 \quad (92)$$

and u, v are viewed as the basis of $(\mathbb{Z}^2)^*$ dual to the standard basis for \mathbb{Z}^2 . In particular, we view $(1, 0)$ as the solution of the equation

$$Q_{a,b,t}(u, v) = 1 \quad (93)$$

which is often called the Thue-equation associated to $Q_{a,b,t}(u, v)$. It is merely a reformulation of κ we introduced earlier, but in this way the argument becomes more natural.

Naturally $\text{GL}_2(\mathbb{Z})$ acts on $\mathbb{Z}^2 \times \text{Sym}^4(\mathbb{Z}^2)^*$, and the action preserves solutions of the Thue-equations. That is to say, the subset

$$\{((n, m), Q(u, v)) \in \mathbb{Z}^2 \times \text{Sym}^4(\mathbb{Z}^2)^*: Q(n, m) = 1\} \quad (94)$$

is preserved by the action of $\text{GL}_2(\mathbb{Z})$.

Proposition 6.1. *The map*

$$\phi: \{(E, t): t \in E(\mathbb{Z})\}/\{\pm 1\} \rightarrow \{((n, m), Q(u, v)): Q(n, m) = 1\}/\sim \quad (95)$$

is injective, where \sim denotes the equivalence relation induced by the action of $\text{GL}_2(\mathbb{Z})$.

Proof. Suppose that two pairs $(Y_{a,b}, t)$ and $(E_{a',b'}, t')$ have the same image under ϕ . Then we have $\gamma \in \text{GL}_2(\mathbb{Z})$ which fixes $(1, 0)$, and transforms

$$Q_{a,b,t} = u^4 - 6x_t u^2 v^2 - 8y_t u v^3 - (3x_t^2 + 4a)v^4 \quad (96)$$

into

$$Q_{a',b',t'} = u^4 - 6x_{t'}u^2v^2 - 8y_{t'}uv^3 - (3x_{t'}^2 + 4a')v^4. \quad (97)$$

It is easy to see that the identity and $(u, v) \mapsto (\pm u, \pm v)$ is only possibility for γ . Indeed, the stabiliser of $(1, 0)$ in $\text{GL}_2(\mathbb{Z})$ is generated by the group of unipotent matrices, together with the transformation $(u, v) \mapsto (\pm u, \pm v)$. By comparing the coefficient of u^3v , one sees that γ must be of the form $(u, v) \mapsto (\pm u, \pm v)$. Thus we conclude that $a = a'$, $b = b'$, and $t = \pm t'$. Of course, $t = \pm t'$ refers to the equality in the Mordell-Weil group of the underlying elliptic curve. \square

Remark 6.1. Note that the two pairs

$$((n, m), Q(u, v)) \sim ((-n, -m), Q(u, v)) \quad (98)$$

are equivalent via the matrix with -1 's on the diagonal.

We briefly recall the invariant theory of binary quartic forms. Let

$$Q = c_0u^4 + c_1u^3v + c_2u^2v^2 + c_3uv^3 + c_4v^4 \quad (99)$$

be a binary quartic form with integer coefficients. With respect to the action of $\text{GL}_2(\mathbb{Z})$, there are two invariants

$$J_2 = \frac{1}{12}c_2^2 - \frac{1}{4}c_1c_3 + c_0c_4 \quad (100)$$

$$J_3 = \frac{1}{216}c_2^3 - \frac{1}{48}c_1c_2c_3 + \frac{1}{16}c_0c_3^2 + \frac{1}{16}c_1^2c_4 - \frac{1}{6}c_0c_2c_4 \quad (101)$$

of degree two and three respectively. We define height of Q as

$$H(Q) = \max \{ 2^6 3^4 \cdot |J_2|^3, 2^{10} 3^{12} \cdot J_3^2 \} \quad (102)$$

where the coefficients in front of $|J_2|^3$ and J_3^2 are chosen so that our definition of height agrees with that of [5].

Proposition 6.2. *Let $t \in Y_{a,b}(\mathbb{Z})$, and $\phi((Y_{a,b}, t)) = (L, Q)$. Then, we have*

$$H(Y_{a,b}) = H(Q). \quad (103)$$

In other words, ϕ preserves the heights.

Proof. This follows from the straightforward calculation. Indeed, Q is given by

$$Q = u^4 - 6x_tu^2v^2 - 8y_tuv^3 - (3x_t^2 + 4a)v^4 \quad (104)$$

and we have the relation $y_t^2 = x_t^3 + ax_t + b$, from which one deduces $J_2(Q) = 4a$ and $J_3(Q) = 4b$. Thus we conclude

$$H(Q) = \max \{ 2^{12} 3^4 |a|^3, 2^{14} 3^{12} b^2 \} = H(Y_{a,b}).$$

\square

Having constructed the injective map ϕ which preserves the heights, the estimation of $N(T)$ is reduced to the estimation of the pairs $((n, m), Q(u, v))$ which lies in the image of ϕ , modulo $\text{GL}_2(\mathbb{Z})$ -equivalence. We consider three types

1. $Q(u, v)$ is irreducible over \mathbb{Q} .
2. $Q(u, v)$ has a linear factor over \mathbb{Q} .
3. $Q(u, v)$ has two irreducible quadratic factors over \mathbb{Q} .

which are mutually disjoint. Let

$$X^i(T) \tag{105}$$

be the GL_2 -orbits of binary forms of type i whose height is less than T .

In each type, we consider three subtypes of $X_j^1(T)$, for $j = 0, 1, 2$, defined by the condition that an element in $X_j^1(T)$ has exactly $4 - 2j$ linear factors over \mathbb{R} .

Theorem 6.2. *We have*

$$\sum_{Q \in X_0^1(T)} 1 = \frac{2\pi^2}{405} T^{5/6} + O(T^{3/4+\epsilon}), \tag{106}$$

$$\sum_{Q \in X_1^1(T)} 1 = \frac{16\pi^2}{405} T^{5/6} + O(T^{3/4+\epsilon}), \tag{107}$$

$$\sum_{Q \in X_2^1(T)} 1 = \frac{4\pi^2}{405} T^{5/6} + O(T^{3/4+\epsilon}), \tag{108}$$

$$\sum_{Q \in X^3(T)} 1 = O(T^{2/3+\epsilon}) \tag{109}$$

where the sum is taken over all irreducible integral binary quartic forms up to $\text{GL}_2(\mathbb{Z})$ equivalence.

Proof. The estimation of the sum over $X_j^1(T)$ is a consequence of Theorem 1.6 of [5]. The estimation of the sum over $X^3(T)$ is given in the proof Lemma 2.3 of [5]. \square

Proposition 6.3. *For $X^2(T)$, we give the following estimation of the sum over the image of ϕ*

$$\sum_{Q \in X^2(T), Q \in \text{Im}(\phi)} 1 = O(T^{3/4}). \tag{110}$$

Proof. If Q is in $X^2(T)$, then Q factors as

$$Q = (u - rv)C(u, v) \tag{111}$$

where r is an integer $C(u, v)$ is binary cubic form with integral coefficients such that $C(1, 0) = 1$. By translation $u \mapsto u + rv$, Q is equivalent to the form

$$u(v^3 + c_1 v^2 u + c_2 v u^2 + c_3 u^3) \quad (112)$$

with integers c_1, c_2 and c_3 . By translating $v \mapsto v + r' u$ for some integer r' if necessary, we may assume that $|c_1| \leq 1$. The invariants of (112) are given as

$$J_2 = \frac{1}{12} c_2^2 - \frac{1}{4} c_1 c_3 \quad (113)$$

$$J_3 = \frac{1}{216} c_2^3 - \frac{1}{48} c_1 c_2 c_3 + \frac{1}{16} c_3^2 \quad (114)$$

and $|J_2| = O(T^{1/3})$ and $|J_3| = O(T^{1/2})$. Hence the discriminant of (112) is $O(T)$. On the other hand, the discriminant is divisible by c_3^2 , hence $|c_3| = O(T^{1/2})$. Now $J_2 = O(T^{1/3})$ together with $|c_3| = O(T^{1/2})$ implies $|c_2| = O(T^{1/4})$. We conclude that there are $O(T^{3/4})$ possibilities for the pair (c_1, c_2, c_3) . \square

We also need to invoke the works of Evertse and Akhtari-Okazaki on the number of solutions of a given Thue-Mahler equations, which we recall now. A Thue-Mahler equation is about a homogeneous binary form $h(u, v) \in \mathbb{Z}[u, v]$ and a finite set S of prime numbers, to which one associates the equation

$$h(u, v) = \pm \prod_{p_i \in S} p_i^{e_i} \quad (115)$$

where e_i are non-negative integers, and u, v are relatively prime integers. A Thue-Mahler equation with $S = \emptyset$ is called a Thue equation. We will rely on a corollary which is easily implied by the following theorem of Evertse.

Theorem 6.3. *Let r be the degree of $h(u, v)$, and assume that $h(u, v)$ has at least three linearly independent linear factors over a sufficiently large number field. Let S be a finite set of prime numbers of cardinality s . Then associated equation (115) has at most*

$$2 \times 7^{r^3(2s+3)} \quad (116)$$

solutions.

Proof. See Corollary 2 of [3]. \square

We are concerned about the case when $h(u, v)$ is a quartic with non-zero discriminant, and S is empty. The following corollary is a direct consequence of Evertse's theorem.

Corollary 6.1. *Let $Q(u, v)$ be a binary quartic form with non-zero discriminant. The equation*

$$Q(u, v) = \pm 1 \quad (117)$$

has at most

$$2 \times 7^{4^3 \cdot 3} < 3.63 \times 10^{162} \quad (118)$$

solutions.

Despite of the large size of the upper bound, we note that it is independent of $Q(u, v)$. On the other hand, we have a significantly better bound due to Akhtari and Okazaki, under the additional assumption that $Q(u, v)$ is irreducible.

Theorem 6.4. *Let $Q(u, v)$ be an irreducible quartic equation. The associated Thue equation*

$$Q(u, v) = \pm 1 \quad (119)$$

has at most 61 solutions, provided that the discriminant of $Q(u, v)$ is greater than an absolute constant, which is effectively computable. Here we regard a solution (n, m) as the same as $(-n, -m)$. If we further assume that $Q(u, v)$ has four linear factors defined over \mathbb{R} , then it has at most 37 solutions.

Now the proof of Theorem 6.1 is straightforward. Indeed, from the injectivity of ϕ , one has

$$N(T) \leq \sum_{Q \in X^1(T)} \sum_{Q(n, m)=1} 1 + \sum_{Q \in X^2(T), Q \in \text{Im}(\phi)} \sum_{Q(n, m)=1} 1 + \sum_{Q \in X^3(T)} \sum_{Q(n, m)=1} 1 \quad (120)$$

where the sum over $Q(n, m) = 1$ means the following: the sum is taken over the set of pairs (n, m) such that $Q(n, m) = 1$, modulo the identification of (n, m) and $(-n, -m)$. Note that (98) shows that two solutions (n, m) and $(-n, -m)$ should be counted once. By Theorem 6.2 and Theorem 6.4, one has

$$\sum_{Q \in X^1(T)} \sum_{Q(n, m)=1} 1 \quad (121)$$

$$= \sum_{Q \in X_0^1(T)} \sum_{Q(n, m)=1} 1 + \sum_{Q \in X_1^1(T)} \sum_{Q(n, m)=1} 1 + \sum_{Q \in X_2^1(T)} \sum_{Q(n, m)=1} 1 \quad (122)$$

$$= 37 \cdot \frac{2\pi^2}{405} T^{5/6} + 61 \cdot \frac{16\pi^2}{405} T^{5/6} + 61 \cdot \frac{4\pi^2}{405} T^{5/6} + O(T^{3/4+\epsilon}) \quad (123)$$

$$< (31.5 \dots) T^{5/6} + O(T^{3/4+\epsilon}) \quad (124)$$

while Theorem 6.2, Proposition 6.3, and Corollary 6.1 imply that

$$\sum_{Q \in X^2(T), Q \in \text{Im}(\phi)} \sum_{Q(n, m)=1} 1 = O(T^{3/4}) \quad (125)$$

$$\sum_{Q \in X^3(T)} \sum_{Q(n, m)=1} 1 = O(T^{2/3+\epsilon}) \quad (126)$$

both of which have smaller orders than $T^{5/6}$. We conclude that

$$N(T) < (31.5 \dots) T^{5/6} \quad (127)$$

for all sufficiently large $T > 0$. Combining with Lemma 6.1, we obtain the desired upper bound on the average number of integral points on $Y_{a,b}$.

References

- [1] S. AKHTARI AND R. OKAZAKI *Quartic Thue equations*, J. Number Theory 130 (2010), no. 1, 40-60.
- [2] L. ALPOGE, *The average number of integral points on elliptic curves is bounded.*, arXiv:1412.1047 [math.NT], 42 pages.
- [3] J.-H. EVERTSE, *On equations in S -units and the Thue-Mahler equation*, Invent. Math. 75 (1984), no. 3, 561-584.
- [4] J.-H. EVERTSE, *The number of solutions of the Thue-Mahler equation*, J. Reine Angew. Math. 482 (1997), 121-149.
- [5] M. BHARGAVA AND A. SHANKAR, *Binary quartic forms having bounded invariants and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) 181 (2015), no. 1, 191-242.
- [6] D. KIM, *A modular approach to Thue-Mahler equations*, arXiv:1501.06274 [math.NT], 42 pages.
- [7] L.J. MORDELL, *Diophantine equations*, Pure and Applied Mathematics, Vol. 30 Academic Press, London-New York 1969 xi+312 pp.
- [8] N.P. SMART, *S -unit equations, binary forms, and curves of genus 2*, Proc. London Math. Soc. (3) 75 (1997), no. 2, 271-307